



(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
26.05.2004 Bulletin 2004/22

(51) Int Cl.⁷: **G06F 1/00**

(43) Date of publication A2:
04.11.1998 Bulletin 1998/45

(21) Application number: **98303173.3**

(22) Date of filing: **24.04.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventors:
• **Takeuchi, Akikazu**
Shinagawa-ku, Tokyo (JP)
• **Nanba, Shinji**
Shinagawa-ku, Tokyo (JP)

(30) Priority: **30.04.1997 JP 11218297**

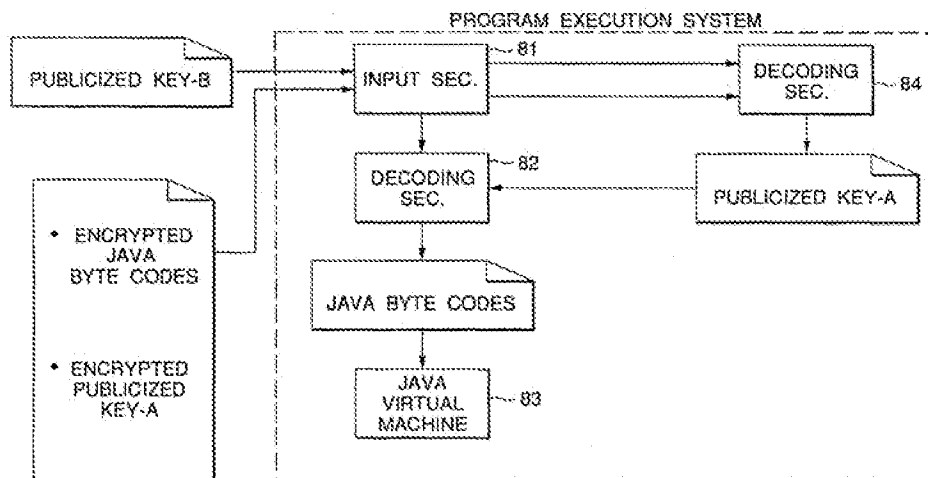
(74) Representative: **Ayers, Martyn Lewis Stanley**
J.A. KEMP & CO.,
14 South Square,
Gray's Inn
London WC1R 5JJ (GB)

(54) **Information processing apparatus and method and recording medium**

(57) In a program execution environment, an application program that was encrypted by using secret key-A is supplied to a decoding section 82, and publicized key-B and an encrypted publicized key-A (corresponding to secret key-A) that was encrypted by using secret key-B corresponding to publicized key-B are supplied to a decoding section 84. The decoding section 84 decodes the encrypted publicized key-A by using publicized key-B and supplies a resulting publicized key-A to

the decoding section 82. The decoding section 82 decodes the encrypted application program by using publicized key that is supplied from the decoding section 84 and supplies Java byte codes as a decoding result to a Java virtual machine 83. The Java virtual machine 83 interprets and executes the Java byte codes that are supplied from the decoding section 82. As a result, it becomes possible to allow only programs developed by a legitimate software developer to be executed in a certain program execution environment.

FIG.1





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 3173

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 706 275 A (IBM) 10 April 1996 (1996-04-10) * abstract *	1-3,5-9	G06F1/00
Y	* page 6, line 40 - page 7, paragraph 1; figures 2-5 *	10-15	
Y	US 4 757 534 A (OSEAS JONATHAN ET AL) 12 July 1988 (1988-07-12) * column 17, line 36 - line 43; claim 1 *	1,2,5-9	
Y	* column 2, line 25 - column 4, line 45 *	3	
Y	EP 0 121 853 A (BURROUGHS CORP) 17 October 1984 (1984-10-17) * page 4, last paragraph - page 5, paragraph 3; claim 12; figure 1 *	1-3,5-9	
Y	* page 8, last paragraph - page 9, paragraph 2 *	10-15 7-9	
A	ANONYMOUS: "Smart Card Protection by the Use of Dynamic Signature Verification One-Way Codes" IBM TECHNICAL DISCLOSURE BULLETIN, IBM CORP. NEW YORK, US, vol. 27, no. 8, 1 January 1985 (1985-01-01), page 4710, XP002195547 ISSN: 0018-8689 * the whole document *	1-3,5-15	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L G06F
A	US 4 168 396 A (BEST ROBERT M) 18 September 1979 (1979-09-18) * abstract; figure 1 *	1-3,5-15	
-/--			
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 26 March 2004	Examiner Beker, H
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application I : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1203 (02.92) (P44031)

Application Number
EP 98 30 3173

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	"SYSTEM FOR M OF M COMPONENT PART RSA DIGITAL SIGNATURE GENERATION" IBM TECHNICAL DISCLOSURE BULLETIN, IBM CORP. NEW YORK, US, vol. 40, no. 4, 1 April 1997 (1997-04-01), pages 1-3, XP000728246 ISSN: 0018-8689 * the whole document *	10-15	
Y,P	BERG C: "How do I create a signed applet?" DR. DOBB'S JOURNAL, M&T PUBL., REDWOOD CITY, CA., US, vol. 22, no. 8, August 1997 (1997-08), pages 109-111,122, XP002140406 ISSN: 1044-789X * the whole document *	10-15	
A,P	SUAN-SUAN CHEW ET AL: "IAuth: An authentication system for Internet applications" COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 1997. COMPSAC '97. PROCEEDINGS., THE TWENTY-FIRST ANNUAL INTERNATIONAL WASHINGTON, DC, USA 13-15 AUG. 1997, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 13 August 1997 (1997-08-13), pages 654-659, XP010247380 ISBN: 0-8186-8105-5 * the whole document *	10-15	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 26 March 2004	Examiner Beker, H
CATEGORY OF CITED DOCUMENTS		T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date O: document cited in the application L: document cited for other reasons A: technological background Q: non-written disclosure P: intermediate document	
X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category			



European Patent
Office

Application Number

EP 98 30 3173

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

- ☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):
- ☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

- ☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.
- ☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.
- ☒ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:
1-3, 5-15
- ☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:



European Patent
Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number

EP 98 30 3173

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-3,5-6,7-9

Information processing apparatus, methods and recording media
for encrypted programs being decrypted using a first and
second key and optionally a third key.

2. claim: 4

Information processing apparatus, methods and recording media
for encrypted programs being decrypted using a plurality of
first keys and a second key

3. claims: 10-15

Information processing apparatus, methods and recording media
for checking program signatures using a first and second key

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 98 30 3173

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-03-2004

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
EP 0706275	A	10-04-1996	CA	2157971 A1	16-03-1996
			EP	0706275 A2	10-04-1996
			US	5956408 A	21-09-1999

US 4757534	A	12-07-1988	CA	1238427 A1	21-06-1988
			DE	3587072 D1	18-03-1993
			DE	3587072 T2	12-08-1993
			EP	0191162 A2	20-08-1986
			JP	1630801 C	26-12-1991
			JP	2060007 B	14-12-1990
			JP	61145642 A	03-07-1986

EP 0121853	A	17-10-1984	CA	1213069 A1	21-10-1986
			EP	0121853 A2	17-10-1984
			JP	59186046 A	22-10-1984

US 4168396	A	18-09-1979	US	4278837 A	14-07-1981

EPO FORM 20489

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82